

Attorney's Docket No.:10559-594001/P12805

Amendment to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method comprising:

determining a private network address for a user in connection with the user accessing a network resource on a network;

determining an access control list entry for the user based on an access control policy;

sending the determined access control list entry from a first computer to a second computer on the network that includes the user and the network resource;

translating a public network address to the private network address for the user accessing the network resource after the access control list entry is sent; and

allowing or blocking the user access based on the access control list entry;

~~wherein determining the access control list entry is performed before translating the public network address to the private network address.~~

2. (Canceled).

Attorney's Docket No.:10559-594001/P12805

3. (Currently Amended) The method of claim 1 2, further comprising:

generating an access control list entry corresponding to the access control policy, that entry including the determined private network address.

4. (Currently Amended) The method of claim 3, wherein the generated access control list entry comprises a network level access control list including at least one of a destination address, a protocol layer designation, a source port, a destination port, the determined private network address, and an indication of allowed or denied access to the network resource.

5. (Currently Amended) The method of claim 1 2, wherein the determined access control list entry comprises an application level access control list entry stored on a storage device connected to the first computer.

6. (Currently Amended) The method of claim 3, wherein determining the private network address comprises allocating a network address based on a dynamic host configuration protocol (DHCP).

Attorney's Docket No.: 10559-594001/P12805

7. (Original) The method of claim 3, wherein the second computer comprises a network layer device, and wherein blocking or allowing access comprises blocking or allowing access at the network layer device.

8. (Currently Amended) The method of claim 5, wherein the second computer comprises a server computer associated with the network resource,

wherein determining an access control list entry further comprises retrieving an application layer access control list entry stored in a database, and

wherein the server computer uses an application layer protocol based on an open system interconnection (OSI) model.

9. (Original) The method of claim 5, further comprising storing the access control policy on a storage medium connected to the first computer in the network, the access control policy including defined roles for each user allowed to access a resource in the network.

10. (Original) The method of claim 3, further comprising: releasing the private network address following completion of the access to the network resource.

Attorney's Docket No.: 10559-594001/P12805

11. (Original) The method of claim 10, further comprising:
de-installing a network layer access control entry
following completion of the access to the network resource.

12. (Currently Amended) An article comprising a machine-readable medium that stores machine-executable instructions, the instructions causing a machine to:

determine a private network address for a user in
connection with the user accessing a network resource on a
network;

determine an access control list entry for the user based
on an access control policy;

send the determined access control list entry from a first
computer to a second computer on the network including the user
and the network resource;

translate a public network address to the private network
address for the user accessing the network resource; and

allow or block the user access based on the access control
list entry after the access control list entry is sent;

~~wherein determining the access control list entry is
performed before translating the public network address to the
private network address.~~

13. (Canceled).

Attorney's Docket No.: 10559-594001/P12805

14. (Currently Amended) The article of claim 12 ~~13~~, further comprising instructions causing a machine to:

generate an access control list entry corresponding to the access control policy, that entry including the determined private network address.

15. (Currently Amended) The article of claim 14, wherein the generated access control list entry comprises a network level access control list including at least one of a destination address, a protocol layer designation, a source port, a destination port, the determined private network address, and an indication of allowed or denied access to the network resource.

16. (Currently Amended) The article of claim 12 ~~13~~, wherein the determined access control list entry comprises an application level access control list entry stored on a storage device connected to the first computer.

17. (Currently Amended) The article of claim 14, wherein determining the private network address comprises allocating a network address based on a dynamic host configuration protocol (DHCP).

Attorney's Docket No.:10559-594001/P12805

18. (Original) The article of claim 14, wherein the second computer comprises a network layer device, and wherein blocking or allowing access comprises blocking or allowing access at the network layer device.

19. (Original) The article of claim 16, wherein the second computer comprises a server computer associated with the network resource,

wherein determining an access control list further comprises retrieving an application layer access control list entry stored in a database, and

wherein the server computer uses an application layer protocol based on an open system interconnection (OSI) model.

20. (Original) The article of claim 16, further comprising storing the access control policy on a storage medium connected to the first computer in the network, the access control policy including defined roles for each user allowed to access a resource in the network.

21. (Original) The article of claim 14, further comprising: releasing the private network address following completion of the access to the network resource.

Attorney's Docket No.:10559-594001/P12805

22. (Original) The article of claim 21, further comprising:
de-installing a network layer access control entry
following completion of the access to the network resource.

23. (Currently Amended) An apparatus comprising:
a first memory that stores executable instructions; and
a first processor that executes the instructions from the
first memory to:

determine a private network address for a user in
connection with the user accessing a network resource on a
network;

determine an access control list entry for the user
based on an access control policy;

send the determined access control list entry to a
second processor on the network including the user and the
network resource;

translate a public network address to the private network
address for the user accessing the network resource; and

allow or block the user access based on the access
control list entry after the access control list entry is sent,

~~wherein determining the access control list entry is~~
~~performed before translating the public network address to the~~
~~private network address.~~

Attorney's Docket No.:10559-594001/P12805

24. (Currently Amended) The apparatus of claim 23, further comprising: the a second processor ~~connected to the first processor, wherein the first processor executes instructions to send the determined access control list entry from the first processor to the second processor in a network.~~

25. (Original) The apparatus of claim 24, wherein the first processor executes instructions to:

generate an access control list entry corresponding to the access control policy, that entry including the determined private network address.

26. (Currently Amended) The apparatus of claim 25, wherein the generated ~~determined~~ access control list entry comprises a network level access control list entry including at least one of a destination address, a protocol layer designation, a source port, a destination port, the determined private network address, and an indication of allowed or denied access to the network resource.

27. (Currently Amended) The apparatus of claim 25, wherein determining the private network address comprises assigning a

Attorney's Docket No.: 10559-594001/P12805

network address based on a dynamic host configuration protocol (DHCP).

28. (Original) The apparatus of claim 25, further comprising:

a storage medium connected to the first processor, wherein the determined access control list entry comprises an application level access control list stored on the storage medium.

29. (Original) The apparatus of claim 24, wherein the second processor comprises a network layer device.

30. (Currently Amended) The apparatus of claim 29, wherein the network layer device executes instructions to block or allow access to the network resource based on the ~~network-level~~ access control list entry.